Network Operations: The Role of the Geographic Combatant Commands

Lieutenant Colonel Peter J. Beim
United States Army

> *Achieving the full potential of net-centricity requires viewing information as an enterprise asset to be shared and as a weapon system to be protected.*
>
> —2006 Quadrennial Defense Review Report

Who decides how the United States deploys information assets, the priority of emplacement of those assets and what actions are taken to secure the Global Information Grid (GIG) and those Joint and Service unique systems riding on it: the Services, the Geographic Combatant Commanders (GCCs), Joint Task Force–Global NetOps (JTF-GNO)? For the last few years that debate has raged in the Network Operations (NetOps) community with the pendulum swinging between a global vice Geographic CCDR focus.

Imagine the following scenario. The United States announces the decision to deploy and begins flowing forces in support of an operation in XCOM's theater.[1] Individual Services begin making decisions on how the information infrastructure will be emplaced to support the operation. An adversary begins to infiltrate key military systems supporting the deployment of military forces. While the adversary is unable to completely mask its efforts, the scope of the intrusion is underestimated as these incidents are all worked within Service channels. Connection requests begin flooding commercial websites, including those that support friendly logistics efforts, rendering them inoperative. XCOM takes action to change the Information Condition in its Area of Responsibility (AOR) affecting systems outside of its theater. A large number of viruses begin to wreck havoc on the Internet and quickly begin to infect Department of Defense (DoD) systems. Discussions begin within the JTF-GNO on whether or not to disconnect the military points of presence from the Internet but the Services raise concerns over the Department's ability to continue to conduct logistical operations with commercial vendors.[2] XCOM is unable to ascertain the status of its theater networks and is worried about whether or not the GIG itself is secure. XCOM becomes concerned over its ability to prosecute the mission assigned to it.

The movement towards a more global control of NetOps, strengthening the overall role of United States Strategic Command (STRATCOM), JTF-GNO, and the Services in NetOps, has limited the Geographic Combatant Command's Command and Control (C2) of NetOps within their AOR. The centralization the Service portions of the GIG impairs the GCC's visibility of the GIG and their ability to support operations within their AOR. This paper will review existing command relationships, Geographic CCDR responsibilities, lines of operations and command relationships; existing and emerging Joint and Service doctrine and specific case studies and lay out recommendations for the role of the Geographic Combatant Command in NetOps C2.

The NetOps Environment

Command and Control of NetOps is a concept that has been evolving over the past decade. Each of the Services, the GCCs and the JTF-GNO has changed their organization and focus for NetOps and each has a stake in the outcome of this issue. To really understand why the NetOps role of the GCCs is an issue, one has to understand where the operations are taking place, what NetOps really is, how each of the organizations involved in NetOps is structured to perform their mission and the current C2 constructs.

Just what are we talking about; what is the GIG? As defined by DoD Directive 8100.1, it consists of the "globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to war fighters, policy makers, and support personnel." This includes government-owned along with leased communications and information systems and services, as well all software, security, services and anything else necessary to operate and secure the GIG, as well as the National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996.[3] By this definition, the GIG encompasses all DoD and National Security information systems at all levels, from tactical to strategic, as well as the interconnecting communications systems.

Most of the discussions on C2 of GIG NetOps center on defense of the GIG network, but NetOps encompass much more than that. NetOps include all actions taken to accomplish the three essential tasks of Enterprise Management, Network Defense, and Content Management, and are intended to provide assured net-centric services across strategic, operational and tactical boundaries in support of DoD's full spectrum of warfighting, intelligence and business missions.[4]

- Enterprise Management is the actual operation of the GIG. It is the technology, processes, and policy necessary to effectively operate the systems and networks that comprise the GIG and includes Enterprise Services Management, Systems Management, Network Management, Satellite Communications Management, and Electromagnetic Spectrum Management.[5]

- Content Management refers to the information itself on the GIG. It ensures information is available to users, operators, and decision makers in a timely manner. Content Management consists of the services that enable discovery, access, delivery, storage and integration of content on the GIG.[6]

- Network Defense is the protection of the GIG and all of the information that moves and resides on it. It is the policies, procedures, programs, and operations that protect the GIG and includes interagency coordination as required. It includes responsibilities for Information Assurance, Computer Network Defense, Computer Network Defense Response Actions and Critical Infrastructure Protection in defense of the GIG.[7]

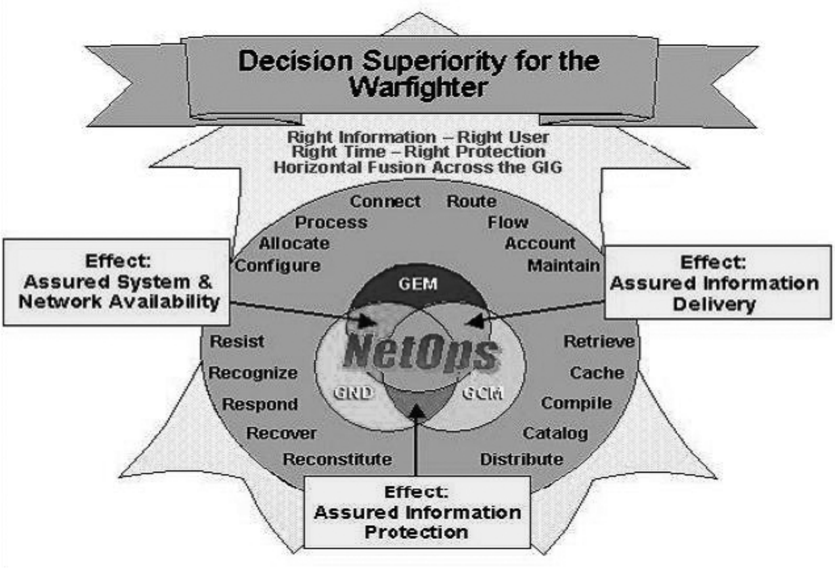

Decision Superiority for the Warfighter
Right Information – Right User
Right Time – Right Protection
Horizontal Fusion Across the GIG
Connect
Route
Process
Flow
Allocate
Account
Configure
Maintain
Effect: Assured System & Network Availability
Effect: Assured Information Delivery
GEM
NetOps
GND
GCM
Resist
Recognize
Respond
Recover
Reconstitute
Retrieve
Cache
Compile
Catalog
Distribute
Effect: Assured Information Protection

Figure 1: JTF-GNO NetOps Construct[8]

Now that the basic constructs of NetOps have been reviewed, the next step is to look at how each of the organizations involved in NetOps is structured to perform their mission. The key players in this discussion are the Services, the Geographic Combatant Commanders (CCDRs) and the JTF-GNO. All have been evolving their structures to meet the changing requirements as well as the changing threat.

The Services have been developing their NetOps missions and structures to meet the growing requirement for bandwidth, access to information, and control and defense of their portion of the GIG. Ten years ago all of the Services maintained some variation of regional control of their NetOps, but that has evolved into more centralized control. The Services have not implemented nor centralized NetOps in the same way. It is essential to understand how they are structured in order to understand why C2 of NetOps has become contentious.

Army NetOps Command and Control

The Army's focus has changed the least of all the Services. The Army continues to maintain organizations, now called the Theater NetOps and Security Centers (TNOSC), which are responsible for NetOps in each GCC. The Army operates a single Global NetOps and Security Center (GNOSC) to which all the TNOSC report. The GNOSC has Technical Control (TECHCON) of all of the TNOSCs, but the TNOSCs belong to the Geographic CCDRs and are controlled by the Theater Network Command, typically the theater signal brigade under the control of the Army Service Component Command in the theater.

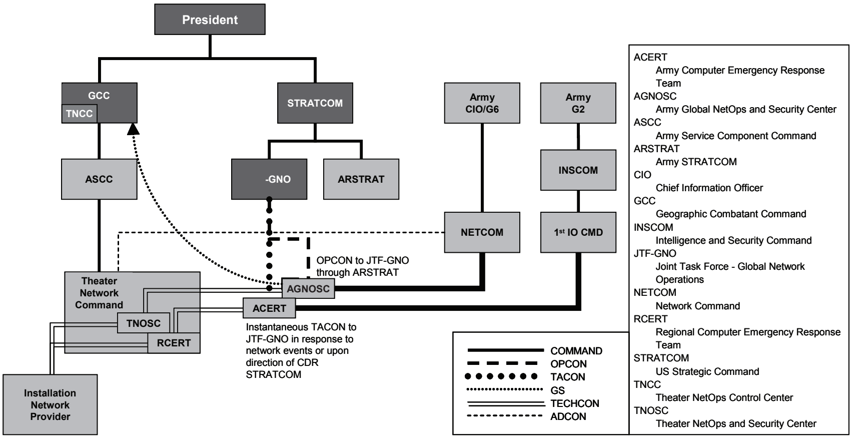

President
GCC
TNCC
STRATCOM
Army CIO/G6
Army G2
ASCC
-GNO
ARSTRAT
INSCOM
NETCOM
1st IO CMD
OPCON to JTF-GNO through ARSTRAT
Theater Network Command
AGNOSC
ACERT
TNOSC
RCERT
Instantaneous TACON to JTF-GNO in response to network events or upon direction of CDR STRATCOM
Installation Network Provider
COMMAND
OPCON
TACON
GS
TECHCON
ADCON
ACERT
Army Computer Emergency Response Team
AGNOSC
Army Global NetOps and Security Center
ASCC
Army Service Component Command
ARSTRAT
Army STRATCOM
CIO
Chief Information Officer
GCC
Geographic Combatant Command
INSCOM
Intelligence and Security Command
JTF-GNO
Joint Task Force - Global Network Operations
NETCOM
Network Command
RCERT
Regional Computer Emergency Response Team
STRATCOM
US Strategic Command
TNCC
Theater NetOps Control Center
TNOSC
Theater NetOps and Security Center

Figure 2: Army NetOps Structure[9]

The GNOSC provides NetOps Enterprise technical direction to the respective theaters while there is a theater NetOps presence that directs/controls NetOps in that theater. U.S. Army Network Command/9th Signal Command has technical and administrative control of the GNOSC, but the GNOSC is under operational control (OPCON) of STRATCOM through its Army element.

Air Force Command and Control

Taking a different approach, the Air Force has shifted its emphasis away from Major Command (MAJCOM) NetOps and Security Centers (NOSCs) to Integrated NetOps and Security Centers (I-NOSCs). Unlike the Army whose TNOSC are in each of the Geographic CCDR's theater and are assigned and report to the Geographic CCDR, the Air Force's I-NOSCs are not one for one with the Geographic CCDRs and report only to the Air Force NetOps Center (AFNOC) which is the Air Force version of the GNOSC. The Air Force realizes that the

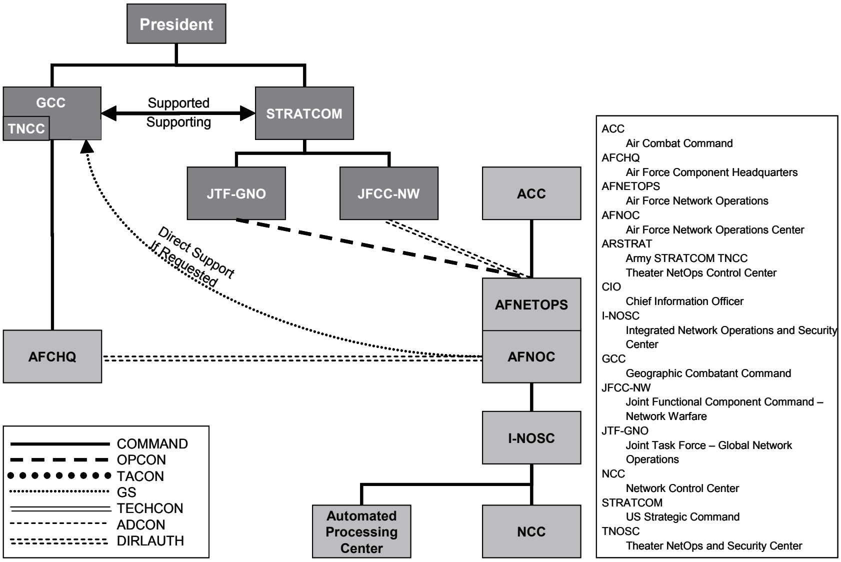

President
GCC
TNCC
Supported
Supporting
STRATCOM
JTF-GNO
JFCC-NW
ACC
Direct Support
If Requested
AFNETOPS
AFCHQ
AFNOC
I-NOSC
Automated Processing Center
NCC
COMMAND
OPCON
TACON
GS
TECHCON
ADCON
DIRLAUTH
ACC
Air Combat Command
AFCHQ
Air Force Component Headquarters
AFNETOPS
Air Force Network Operations
AFNOC
Air Force Network Operations Center
ARSTRAT
Army STRATCOM TNCC
Theater NetOps Control Center
CIO
Chief Information Officer
I-NOSC
Integrated Network Operations and Security Center
GCC
Geographic Combatant Command
JFCC-NW
Joint Functional Component Command – Network Warfare
JTF-GNO
Joint Task Force – Global Network Operations
NCC
Network Control Center
STRATCOM
US Strategic Command
TNOSC
Theater NetOps and Security Center

Figure 3: Air Force NetOps Structure[10]

Geographic CCDR must still be able to direct network activities within their AOR and has established a General Support relationship between the AFNOC and each GCC and established dedicated GCC liaison cells within the AFNOC.[11] Additionally, the Air Force has given the MAJCOMs the latitude to establish Communications Control Centers in their theaters to serve as the focal point for interaction between AFNOC and their respective CCDR.[12]

Navy NetOps Command and Control

The Navy, like the Air Force, has moved away from a regional focus to their NetOps. They have replaced their regional Navy Computer and Telecommunications Master Stations (NCTMS) with two Regional NOSCs (RNOSCs) under the Navy GNOSC (NAVGNOSC) to support all Navy NetOps world-wide. As much of their NetOps is conducted afloat, the Navy has established the Fleet NetOps Centers (NOCs), collocated with the two RNOSCs in the continental United States (CONUS) or with the NCTMS located in Naples and Bahrain. The Fleet NOCs are the tactical entry points for fleets operating in their operations area and provide them with all voice, video, data and network services, passing the fleet from one Fleet NOC to the next

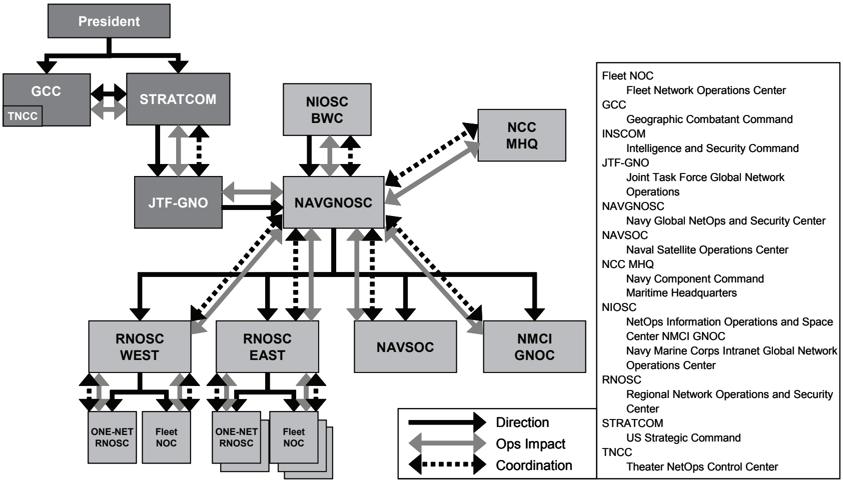

President
GCC
TNCC
STRATCOM
NIOSC BWC
NCC MHQ
JTF-GNO
NAVGNOSC
RNOSC WEST
RNOSC EAST
NAVSOC
NMCI GNOC
ONE-NET RNOSC
Fleet NOC
ONE-NET RNOSC
Fleet NOC
Direction
Ops Impact
Coordination
Fleet NOC
Fleet Network Operations Center
GCC
Geographic Combatant Command
INSCOM
Intelligence and Security Command
JTF-GNO
Joint Task Force Global Network Operations
NAVGNOSC
Navy Global NetOps and Security Center
NAVSOC
Naval Satellite Operations Center
NCC MHQ
Navy Component Command Maritime Headquarters
NIOSC
NetOps Information Operations and Space Center NMCI GNOC
Navy Marine Corps Intranet Global Network Operations Center
RNOSC
Regional Network Operations and Security Center
STRATCOM
US Strategic Command
TNCC
Theater NetOps Control Center

Figure 4: Navy NetOps Structure[13]

as it transits their operating areas.[14] The majority of their unclassified networks are run by contractors either under the Navy Marine Corps Internet (NMCI) contract in CONUS or the outside of CONUS (OCONUS) Navy Enterprise Network (ONE NET). To deal with this in the United States, the Navy established the NMCI Global NetOps Center (GNOC) to provide operational direction to the NMCI contractor for the Navy portion of the NMCI. OCONUS, they established TNOSCs that report directly to the RNOSCs responsible for their respective area. These TNOSCs are not assigned to the GCC in whose theater they operate.[15]

The basic organization to support global Navy NetOps is the NAVGNOSC and the East and West RNOSCs. The NAVGNOSC integrates separate common operational pictures from the Navy RNOSCs, the NMCI GNOC, and the Naval Satellite Operations Center (NAVSOC) to provide global C2 for networks and situational awareness to the JTF-GNO.[16] The Navy, unlike the Army, does not maintain a NetOps force assigned to the GCC. The support relationship established by JTF-GNO between the Services and the GCC does not enable the GCC to direct actions on the Navy portion of the GIG in their AOR. Any actions the GCC requires must be requested through the NAVGNOSC.

Geographic Combatant Command NetOps Command and Control

While none of the GCCs are organized exactly the same for NetOps within their AOR, they all have the same basic characteristics. Each GCC has established a Theater NetOps Control Center (TNCC) and has a Theater NetOps Center (TNC) run by Defense Information Systems Agency (DISA). None of the TNCCs are identical. U.S. Central Command (CENTCOM) has combined their TNCC with the DISA TNC and dubbed it the Central Region Theater NetOps Center while U.S. European Command (EUCOM) established a Theater Communication Control Center, which works for the J3 instead of the J6.[17, 18] But even with these differences, all the TNCCs are used by the GCCs for the C2 of the portion of the GIG in their AOR (also referred to as the Theater Information Grid [TIG]).

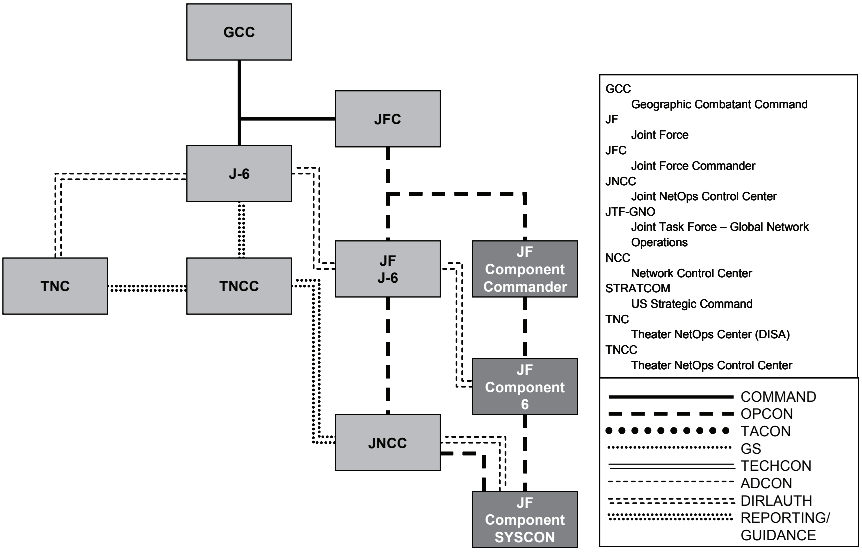


Figure 5: GCC NetOps Structure[19]

The TNCCs are the CGG's lead for prioritizing and directing theater GIG assets and resources in support of their missions and are the theater interface with DISA, the Services and JTF-GNO.[20] They monitor the status of their TIG through interaction with the TNC and the TNOSCs and determine the operational impact of proposed JTF-GNO actions. The TNCCs determine the operational impact of major degradations and outages, and lead and direct TNC and TNOSCs responses to them in support of operational priorities. When there are no Service TNOSCs in Theater, the TNCC coordinates directly with the Service GNOSC for actions required by the GCC.

U.S. Northern Command (NORTHCOM) is in a unique position. While it is a GCC with an assigned AOR, most of the forces within its AOR, to include the NetOps forces, do not belong to NORTHCOM, but rather belong to U.S. Joint Forces Command (JFCOM) for Global Force Management. NORTHCOM does have a TNCC and component forces like the other GCCs, but those component forces have not established TNOSCs and so NORTHCOM must rely on the General Support provided by the Service NOSCs. This leaves NORTHCOM in a position where it is responsible for conducting operations within its AOR, but does not have visibility on its TIG nor the authority to direct actions on it.

STRATCOM NetOps Command and Control

Just as the Services and Combatant Commands have evolved their NetOps constructs, so has the DoD. For many years, there was no centralized control of Department NetOps. But in 1997 the Department conducted the Eligible Receiver exercise and found DoD networks vulnerable and the Combatant Commands, Services and Defense Agencies (CC/S/A) unable to coordinate a response.[21] That prompted the DISA to create an entity that would eventually become today's JTF-GNO charged with the operations and defense of the GIG.

JTF-GNO's C2 of NetOps has likewise developed. Prior to the current Unified Command Plan (UCP), C2 of NetOps was in the hands of the CCDRs who had oversight of component network management capabilities, while providing situational awareness of the GIG.[22] The initial version of the NetOps concept of operations (CONOPS) continued to focus on GCC control of NetOps within their AOR, stating that for theater issues, "Combatant Commanders will exercise their authority over forces assigned, including the authority to prioritize and direct changes in the GIG where and when appropriate in support of their missions....Combatant Commanders will exercise OPCON of their assigned NetOps forces and TACON of the TNC

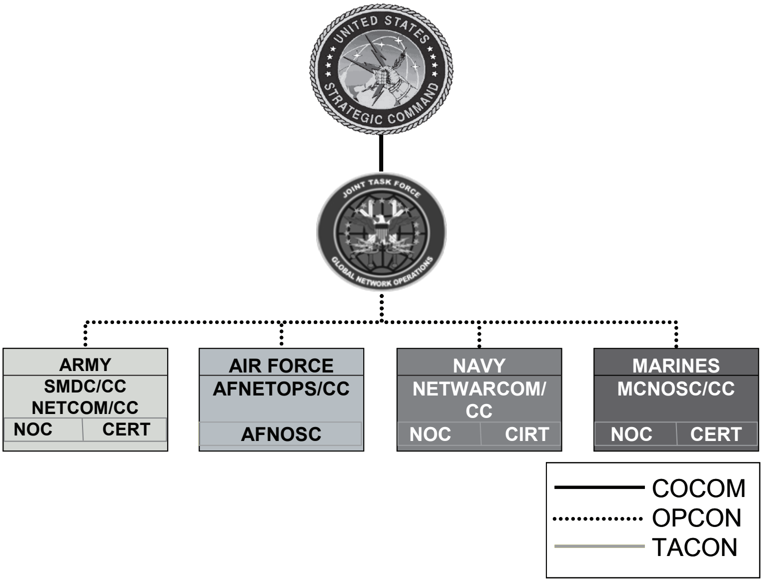


Figure 6: JTF-GNO NetOps Structure[23]

for Theater NetOps issues and will establish operational priorities for and assessments of NetOps actions in support of their missions."[24] Even for global issues, the initial CONOPS had JTF-GNO directing actions through the TNCCs of the Geographic CCDRs.

Subsequent versions of the CONOPS changed that focus. JTF-GNO has moved to a more global C2 architecture, strengthening the overall role of STRATCOM, JTF-GNO, and the Services in NetOps. JTF-GNO established three situational constructs in the CONOPS for NetOps C2: Global, Theater, and Non-Global. The determination of which construct to use is based on entities affected and the capability of the theater affected. This C2 structure is applied by event and leads to the possibility of a Geographic Combatant Command with multiple NetOps events occurring being simultaneously supported and supporting; sometimes in the chain of command for what is occurring and sometimes bypassed.[25]

Global Events

Global Events are activities that have the potential to affect the operational readiness of the GIG writ large and require coordination between affected CC/S/A.[26] The Strategic Command (STRATCOM)

Commander has the discretion to declare an event global any time activities cross a Geographic Combatant Command boundary, affects multiple combatant commands, affects other DoD Agencies or is beyond the GCC's capabilities.[27] Global Events include rapid spread of malicious code, allocation of satellite commuications (SATCOM) capabilities, loss of enterprise applications or any other NetOps event clearly not restricted to a single theater.

For Global Events STRATCOM is the supported command, issuing orders and direction through JTF-GNO to the CC/S/As.[28] JTF-GNO tasks its Service NetOps components to support the execution of global NetOps and issue direction directly from JTF-GNO to their respective Service NetOps forces around the globe. It is important to note that this direction does not go through the GCCs to the NetOps forces in their theaters.

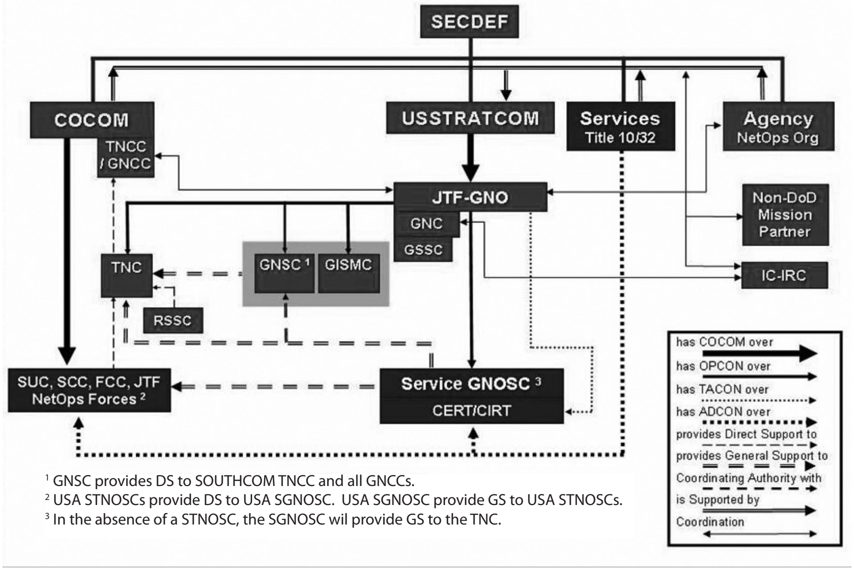

SECDEF
COCOM
TNCC / GNCC
USSTRATCOM
Services
Title 10/32
Agency
NetOps Org
JTF-GNO
GNC
GSSC
Non-DoD Mission Partner
IC-IRC
TNC
GNSC 1
GISMC
RSSC
SUC, SCC, FCC, JTF NetOps Forces 2
Service GNOSC 3
CERT/CIRT
has COCOM over
has OPCON over
has TACON over
has ADCON over
provides Direct Support to
provides General Support to
Coordinating Authority with
is Supported by
Coordination
1 GNSC provides DS to SOUTHCOM TNCC and all GNCCs.
2 USA STNOSCs provide DS to USA SGNOSC. USA SGNOSC provide GS to USA STNOSCs.
3 In the absence of a STNOSC, the SGNOSC wil provide GS to the TNC.

Figure 7: JTF-GNO C2 for Global Events[29]

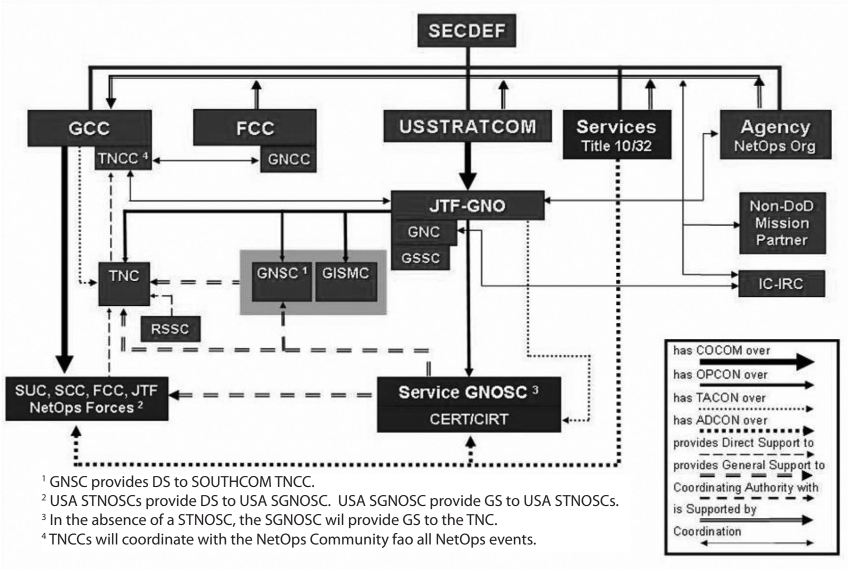
While this supported relationship gives the STRATCOM Commander global authority, the CONOPS is quick to point out that it does not negate the CCDR's authority over NetOps forces assigned in the UCP.[30] JTF-GNO Service NetOps components are tasked to support the execution of operating and defending against global and non-global NetOps events, while synchronizing actions with affected

CCDRs and their respective components.[31] The CONOPS requires the CC/S/As to lead their respective responses to global NetOps events in accordance with STRATCOM and JTF-GNO direction.[32]

The CONOPS, as well as historical data maintained by JTF-GNO, acknowledges that most NetOps events begin in a local enclave that is under the control of the respective Geographic CCDR.[33] Properly handled at the local level, these events never become Global Events.

Theater Events

Theater Events are activities occurring within a theater that have the potential to affect the operations in only that theater. This is the major distinction between Global and Theater Events. The affected GCC becomes the supported command for all activities related to that event and STRATCOM assumes the role of a supporting command.[34] JTF-GNO Service NetOps components provide support to the GCC through their Service TNOSCs. If a Service does not have a TNOSC, the Service GNOSCs provides General Support (GS) to the TNCC. Providing General vice Direct Support means the GCC cannot direct actions of the Service GNOSCs on actions to take in their theater.[35]



[1] GNSC provides DS to SOUTHCOM TNCC.
[2] USA STNOSCs provide DS to USA SGNOSC. USA SGNOSC provide GS to USA STNOSCs.
[3] In the absence of a STNOSC, the SGNOSC wil provide GS to the TNC.
[4] TNCCs will coordinate with the NetOps Community fao all NetOps events.

Figure 8: JTF-GNO C2 for Theater Events[36]

Non-Global Events

Non-Global Events are activities that affect Functional Combatant Commands, unassigned Title 10 Service forces or defense agencies. Since these forces have no AOR of their own, these events are considered neither global nor theater in nature. For Non-Global Events, Commander STRATCOM is the supported commander and JTF-GNO provides GS to the affected Functional CC/S/As as required. Non-Global Events most often occur within U.S NORTHCOM's AOR because that is where the affected forces and organizations are located. For the purposes of C2 discussions, Non-Global Events are the same as Global Events.[37]

Competing C2 Requirements

Service Requirements

Although there is not one single consolidated Service position, there is a consistent theme between the Services for the most efficient and cost-effective method of controlling their NetOps. Services, in accordance with their Title X responsibilities, have established unique networks, applications, and tools in support of their needs and connected them to the GIG. Each of the Services has a responsibility to operate their portion of GIG and this requires some degree of centralization of their NetOps along Service lines in order to achieve the desired efficiencies and fiscal return on investment.

The primary argument for centralizing control of the GIG is the global nature of NetOps. The Department's net-centric goals of improved military situational awareness and significantly shortened decision-making cycles can only be achieved through horizontal fusion of the networks and enterprise services all of which requires centralized control.[38] The most recent Quadrennial Defense Review report points to the need to "cut across legacy stove-piped systems" in order to achieve net-centricity.[39]

To make the best use of scarce resources, they must be committed when and where needed and this requires a global focus. Allocation of satellite bandwidth, Standardized Tactical Entry Point sites, bandwidth, and NetOps forces themselves to support a particular mission must be done with an understanding of the global implications. From a Service perspective, centralization and enterprise management flattens the force structure required to operate and defend their networks.

Combat operations conducted by Geographic CCDRs no longer occur strictly within their own AOR. Ground forces in combat routinely reach back to remote Unmanned Aerial Vehicle pilots in CONUS to direct aircraft in support of their operations.[40] As the Prompt Global Strike program develops, commanders will be able to call for conventional strikes by weapons systems based far outside of their Area of Operation (AO).[41]

The Navy points out that its very nature is global and it has units constantly crossing Combatant Command boundaries. A Carrier Strike Group when deployed, for example, may not be all in one theater at all times. Additionally, actions taken by CCDRs on a theater level can have global implications. A change in network defense posture may have staggering financial costs for a Service Internet, but Combatant Commands may not have visibility on these kinds of ramifications.[42]

The nature of the threat to DoD networks is global as well. An enemy cannot easily attack physical infrastructure on opposite sides of the globe. In cyberspace, that occurs routinely. Information on attacks must be shared rapidly globally to ensure that methods used by attackers can be identified and defended against throughout the GIG. Intrusions, even failed intrusions, which may seem trivial on an individual basis, may show a larger pattern of intent when laid against the global backdrop of the GIG. Virus outbreaks by their very nature have global implications for the GIG. Once again, failure to recognize the global implications can have significant impact.[43]

The Navy stresses that there is no such thing as a theater view; all efforts in regards to NetOps must be global.[44] Their argument is that in fighting the network there are no geographic boundaries, the battlespace is shared by all of the DoD equally, and that to gain information superiority the DoD must be able to maneuver and mass effects by sharing information rapidly and globally.

Additionally, both the Air Force and Navy point out that NetOps forces are not apportioned to the CCDRs. Neither the Air Force nor the Navy has NetOps organizations (e.g. Service TNOSC) in a CCDR's AOR and the majority of their NetOps forces in a theater are simply installers and maintainers. Finally, they both note that the only reference in official documents to a CCDR with responsibility for the GIG is STRATCOM.

GCC Requirements

For the GCCs there are two main concerns regarding C2 of NetOps. First is the need for timely control of their TIG. Second is the need to operate their network as a weapon system to allow commanders to fight the network jointly through the full spectrum from routine daily operations to full-scale combat.

The Services, in the conduct of their Title X duties, have developed Service-unique solutions to support Service-unique missions. Each Service or agency organizes their NetOps forces in the manner they believe provides the most effective and efficient use of scarce resources. The GIG, however, is not a Service specific construct but a joint construct. The stove-piped systems and the method by which Services are deploying them degrade the effectiveness of the TIGs. When the Army developed a secure Internet Protocol (IP) phone solution, Secure Voice over IP (S-VoIP), ahead of the rest of the DoD and deployed it, it could not, for security reasons, be connected to the secure IP phone solution, Voice over Secure IP (VoSIP), adopted by the rest of the Department. This created two separate secure IP voice solutions that cannot connect within the Combatant Command AOR. The CCDR had to mandate disconnecting the Army S-VoIP within their AOR to ensure there would be a single, interoperable solution; but this solution precludes Army units in theater using a secure IP phone to talk to Army units outside of the theater.[45]

Several bases in a Combatant Command AOR serve multiple Services and agencies. There are multiple examples where the tenants have set up duplicative capabilities (satellite terminals, tech control facilities, etc.) on the same base with no interconnection. Situations abound where data sent from one side of a base to the other has to travel back to CONUS first before being delivered to its recipient two miles away from the sender. Fiber cables are laid right next to one another and travel identical paths between buildings, but not interconnected because they belong to different Services or agencies. The CCDR has had to direct a solution to get the interconnectivity because the Services and agencies in theater are not operating jointly.[46]

Centralization of the Service's NetOps forces needs to be transparent to the GCCs and not impair their ability to conduct operations and direct action on the network when required. The Services must be able to effectively prioritize and react to direction from multiple supported Combatant Commands just as they did when the Services maintained NetOps forces in theater. The situation is exacerbated as forward-deployed forces become more dependent upon capabilities provided via reach-back over the GIG. The ability of the CCDR to orchestrate effects and fight the network is impaired when centralization causes Services' forces to be unable or unwilling to respond to the requirements of the CCDR.[47]

During the humanitarian assistance operation Unified Endeavor, conducted in the wake of the 2004 Tsunami, Pacific Command (PACOM) released direction to assigned forces to take specific network defense actions in preparation for the planned operation. The centralization of many Navy and Marine NetOps and defense functions at the Navy Global NetOps Centers made some relatively straightforward network defense measures beyond the ability of PACOM's assigned Marine and Navy forces to implement, thus increasing risk to PACOM and global networks and operations."[48]

The Combatant Commands are concerned that the increasing emphasis on centralized Service control of the GIG is degrading their ability to see and fight their portion of the GIG. With combat forces it is clear when a unit is training or conducting other functions under Service authority and when it is engaged in combat or other operations under the CCDR's authority.[49] The ability to command the forces operating in the information domain is as important as the ability to command forces in the air, land, sea and space domains. For command, control, communications and computer systems (C4S) and networks, as well as the forces that operate and defend them, the dual and in some cases triple reporting chains make it unclear who is actually in charge at what point in the fight. During Global or Non-Global Events, the CCDRs are bypassed altogether and JTF-GNO operates directly through the Services. Though the Joint NetOps CONOPS is very specific about the requirement to coordinate actions with the CCDRs, in a fluid, fast-moving environment, that requirement can quickly become an afterthought.[50]

Information Assurance Vulnerability Alerts, Computer Tasking Orders and changes to Information Conditions issued outside of the Combatant Command are an example of this issue. These actions have direct influence on operations being conducted by the CCDRs in their theaters. When the Services try to direct actions on these Information Assurance Vulnerability Alerts and Computer Tasking Orders at an enterprise level, they cannot discern the affect on the CCDRs operations with respect to the manner and timing of the implementation. Only the CCDR has the insight to be able to do this. When a security threat triggered the Air Force Space Command to request an computer defensive status change the Air Force coordinated the action with JTF-GNO but did not notify or coordinate with NORTHCOM resulting in a significant challenges to NORTHCOM.[51]

In CENTCOM, this lack of control of NetOps forces within their theater affects their ability to ensure network availability to the commander when needed. The Navy operates numerous portions of the CENTCOM TIG. The Navy NetOps forces in the AO do not work for the Navy element of CENTCOM and report only to Navy Regional NetOps and Security Center West. The CENTCOM Central Region Theater NetOps Center, which is charged with maintaining and directing all NetOps actions for the CCDR, is not in the Navy NetOps forces reporting chain, so often does not have full situational awareness of all that is happening on the CENTCOM TIG. Workarounds have been established to address this issue, but no formal solutions are in place.[52]

For NORTHCOM, this lack of OPCON of NetOps forces created a significant predicament during relief efforts for Hurricane Katrina in 2005. During the operation, equipment from the Services flowed into Joint Operations Area (JOA) without approval and authority to operate.

This caused significant spectrum management and operational issues as NORTHCOM did not have visibility over what was flowing into the JOA and was unable to provide guidance or coordinate actions.[53]

While the Services are generally advocating a more centralized structure under JTF-GNO, it is worth noting that the Combatant Command that has been given responsibility for operation and defense of the GIG, STRATCOM, is not pushing for that centralized structure. In fact, STRATCOM has been instrumental in maintaining the GCC's role in NetOps with their Theater and Global Event construct and emphasis throughout the latest round of briefing on NetOps to the Joint Staff.[54]

Both the Services and the Combatant Commands are looking to centralize control of NetOps at the Joint level. The key questions that arise are:

- Who is in charge?
- At what level does centralization of NetOps take place: the Global level, Theater level or some other level?
- Are network effects simply a service that the CCDRs go to JTF-GNO to request or do the CCDRs have the need to direct and prioritize actions for networks within the theater?

In the end, the CCDRs are the ones charged by the President with accomplishing the Nation's military missions within their AOR.[55] Forces assigned to the CCDR are under their authority to accomplish those missions. There is no argument with this from those advocating a global control as they point to the fact that NetOps forces are under the control of STRATCOM.

But the GIG is now a key part of the CCDR's C2 capability; the commander's ability to conduct military operations. Without the GIG aircraft don't fly, ground units don't move, ships don't sail, and satellites don't provide information. Just as commanders need to be able to direct their combat forces and know their locations and status, they need to have control over the GIG and know its status. They must be able to see the scope, capability and status of their TIG; must be able to see how events outside of their theater affect their TIG; and must be able to direct and prioritize actions in order to support their operations. If we truly believe the rhetoric about fighting the network, then CCDRs, not a centralized enterprise management operations center, must be given the appropriate control to conduct operations.

And, as long as the GCC structure remains in place, all missions conducted, even those by the Functional Combatant Commands, will occur in the Geographic CCDR's AOR. All aspects of NetOps have a physical component to them. Network Operation actions will affect those CCDRs and their operations. At the same time centralization is necessary to achieve the goals of net-centricity, to be able to effectively defend the network and to rapidly mass effects. This concept of centralization is not mutually exclusive from the need for the Geographic CCDRs to prioritize and direct their TIG.

Way Ahead

To achieve a viable NetOps C2 construct requires striking a balance between the needs of the Geographic CCDRs and the need to establish centralized control of the GIG. The current evolution of the Joint NetOps CONOPS and the transformation of the Services NetOps forces, organization and doctrine need to be leveraged to achieve that balance. To do this, the DoD should undertake the following:

- Create a single, unambiguous chain of command for NetOps making STRATCOM the supported command for all NetOps. This will answer the key question of who is in charge. Situational C2 constructs only add to the fog of war in what is already a fast-paced and fluid environment. A single chain of command will ensure that NetOps forces know whom they take direction from and whom they report to and this chain of command must include the GCCs.
- Give the GCCs authority over NetOps within their AOR by:
  – Modifying the UCP to give responsibility for NetOps within their AOR to the Geographic CCDR.
  – Modifying the existing GIG NetOps CONOPS to specify that Services without a Service TNOSC in the theater provide direct support from their GNOSC to the GCC.

  – Specifying that all directives issued from JTF-GNO go to the GCCs for execution.

These changes will ensure that all elements in the theater respond to only one chain of command, through the GCCs to STRATCOM. This will also resolve NORTHCOM's dilemma of having responsibility for an AOR but no authority over its NetOps.

- Establish a Joint NetOps Center in each of the GCCs following the CENTCOM model of merging the CCDR's TNCC with JTF-GNO's TNC. This would essentially establish a Joint Component Commander in each of the GCCs for the cyber domain just as one is established for operations on land, air and space, and the sea.[56] To do this, the Combatant Command J-6 would wear two hats; one as the J6 for the Theater under the OPCON of the Combatant Command and the other as the Theater NetOps Authority, in charge of the Joint NetOps Center under the TACON of JTF-GNO.[57] All Service TNOSC would be under the TACON of the Joint NetOps Center. Any Service without a Service TNOSC in the theater would have their GNOSC in direct support of the Joint NetOps Center.
- Refocus centralization of the GIG and make STRATCOM the lead for this effort. The current centralization efforts focus on centralizing Service control of their NetOps and runs counter to the concepts behind net-centricity. Service-centricity creates unnecessary stove-pipes in information and processes and takes us away from the goal of "giving all users access to the latest, most relevant, most accurate information."[58] The Beyond Goldwater-Nichols report makes it clear that management and organization of Command, Control and Communications (which includes NetOps) should be in the hands of the Joint community.[59]

Conclusion

There is a pressing need to centralize C2 of NetOps. Flattening the network allows the DoD to increase efficiency, save costs and manage scarce resources. More importantly, this improves the ability of NetOps forces to manage and securely deliver timely, accurate information to decision-makers enabling them to rapidly mass effects.

This centralization must be balanced against the need for effective C2 of NetOps. The reliance on the GIG for all aspects of warfighting requires that commanders be aware of the status and capabilities of their TIG and be able to reprioritize efforts to support operations.

"[W]e must change the paradigm in which we talk and think about the network; we must fight rather than manage the network, and operators must see themselves as engaged at all times, ensuring the health and operation of this critical weapons system."[60] NetOps are crucial to fighting and winning our Nation's wars, from providing command and control, to reducing the decision cycle, to bringing assets outside of the theater of operations to bear. STRATCOM has made tremendous strides in moving forward the concept of NetOps and those efforts must continue. The Geographic CCDRs must be involved in the operations and defense of their portion of the GIG in order to ensure that we are able to successfully fight the network.

Endnotes

1. XCOM is intended to refer to a notional Geographic Combatant Commander.
2. Joint Task Force–Global Network Operations (JTF-GNO) is charged by U.S. Strategic Command (STRATCOM) with carrying out STRATCOM's mission of operating and defending the Global Information Grid (assigned to STRATCOM in the 2006 Unified Command Plan).
3. U.S. Department of Defense, *Global Information Grid (GIG) Overarching Policy*, Department of Defense Directive 8100.1 (Washington, D.C.: U.S. Department of Defense, September 19, 2002), 8.
4. Net-centric is "relating to or representing the attributes of net-centricity. Net-centricity is a robust, globally interconnected network environment (including infrastructure, systems, processes, and people) in which data is shared timely and seamlessly among users, applications, and platforms. Net-centricity enables substantially improved military situational awareness and significantly shortened decision making cycles. Net-Centric capabilities enable network-centric operations and NCW." U.S. Department of Defense, *Data Sharing in a Net-Centric Department of Defense*, Department of Defense Directive 8320.2 (Washington DC: U.S. Department of Defense, 2 December 2004), 8.
5. Joint Task Force–Global Network Operations, Joint Concept of Operations for Global Information Grid NetOps, ver. 3 (Offutt Air Force Base NE, U.S. Strategic Command, 4 August 2006), 5. This document is referenced hereafter as Joint CONOPS for GIG NetOps, ver. 3.

6. Ibid., 7.
7. Ibid., 6.
8. Ibid., 10.
9. U.S. Department of the Army, *Draft Concept of Operations for LandWarNet (LWN) NetOps (NetOps)* (Washington DC, U.S. Department of the Army, 21 June 2006), 21. This diagram is a modified version of LandWarNet NETOPS Organization Structure. The diagram was modified to make it consistent with the other diagrams within this paper. Note that while this CONOPS is not yet finalized, it is the author's belief the items referenced will not change significantly, and the publication still provides a legitimate, Service-level reference.
10. U.S. Air Force, Air Force NetOps, United States Air Force Network Operations Functional Concept (Langley Air Force Base, VA: U.S. Air Force, Air Combat Command, 12 October 2006), 16. This diagram is a modified version of AFNetOps C2 Structure diagram. The diagram was modified to make it consistent with the other diagrams within this paper.
11. Ibid., 18.
12. Ibid.
13. U.S. Navy, Naval Network Warfare Command, Navy Concept of Operations for Global Network Operations, Version 1.0 (Norfolk VA, Naval Network Warfare Command, September 7, 2006), 13.
14. Ibid., 11.
15. Ibid., 12.
16. Ibid.
17. Lieutenant Colonel Benjamin J. Barris, CENTCOM J6, e-mail message to author, November 21, 2006.
18. Author's personal experience as the EUCOM Theater Network Defense Chief in 2005.
19. U.S. Joint Chiefs of Staff, Joint Communications System, Joint Publication 6-0 (Washington, D.C., U.S. Joint Chiefs of Staff, March 20, 2006), III-2.
20. Joint Publication 6-0, III-1.
21. Hunter Keeter, "DISA Stands Up Computer Network Defense Center," Defense Daily 203, no. 30 (August 12, 1999): 1, www.proquest (accessed October 3, 2006).
22. Deputy Secretary of Defense, "GIG Network Operations," Guidance and Policy Memorandum 10-8460, August 24, 2000, referenced in Joint CONOPS for GIG NetOps, ver. 3: 4.
23. Joint CONOPS for GIG NetOps, ver. 3, 24.

24. Joint Task Force–Global Network Operations, Joint Concept of Operations for Global Information Grid NetOps (Offutt Air Force Base NE, U.S Strategic Command, May 5, 2004), 22. This document is referenced hereafter as Joint CONOPS for GIG NetOps, Version 1.

25. Joint CONOPS for GIG NetOps, ver. 3, 11.

26. Ibid., 2.

27. Ibid., 11.

28. Ibid.,13

29. Ibid., 14.

30. Ibid.

31. Ibid.

32. Ibid.

33. Ibid., 3 and 14.

34. Ibid., 3.

35. General Support is the support provided by the supporting force to the supported force as a whole rather than to a particular subdivision of the supported force. U.S. Joint Chiefs of Staff, Unified Action Armed Forces (UNAAF), Joint Publication 0-2 (Washington DC, U.S. Joint Chiefs of Staff, July 10, 2001), III-10. Direct Support is a mission assigned to a force requiring support to another specific force and authorizing the supporting force to answer directly to the supported force's request for assistance (Ibid). This requirement to respond directly to the supported forces requests is a key distinction between Direct and General Support.

36. Joint CONOPS for GIG NetOps, ver. 3, 15.

37. Ibid., 3.

38. U.S Department of Defense, DoD Chief Information Officer Strategic Plan for Information Resources Management (Washington DC: U.S. Department of Defense, June 2004), 12.

39. U.S Department of Defense, Quadrennial Defense Review Report (Washington DC, U.S. Department of Defense, February 6, 2006), 70.

40. Ibid.

41. Noah Shachtman, "Hypersonic Cruise Missile: America's New Global Strike Weapon," *Popular Mechanics*, January 2007, http://www.popularmechanics.com/technology/military_law/4203874.html (accessed Dec 22, 2006).

42. Lieutenant Commander Julie R. Fluhr, NETWARCOM, N55, e-mail message to author, November 29, 2006.

43. Ibid.

44. Navy response to JTF-GNO's NetOps CONOPS.

45. Barris.

46. Ibid.

47. Colonel Jennifer L. Napper, J6, U.S. Pacific Command, *NETOPS Command and Control; A GCC Perspective* (Camp H.M. Smith HI: U.S. Pacific Command, March 2006), 5.

48. Ibid., 4.

49. Ibid.

50. Brandon Sade, EUCOM J6, e-mail message to author, October 11, 2006.

51. Briefing, NORTHCOM NetOps Discussion Points, 3

52. Barris

53. NORTHCOM Briefing, 4.

54. Briefing, Joint CONOPS for GIG NetOps, 02 Aug 2006, 10-12

55. UNAAF, vii.

56. During joint operations, the Joint Force Commander may set up his force with subordinate land (Joint Force Land Component Commander), air and space (Joint Force Air Component Commander) and sea (Joint Force Maritime Component Commander) commanders as fits his operation.

57. This proposal was adapted from a concept provided to JTF-GNO by EUCOM J-6 in response to the staffing of Joint CONOPS for GIG NetOps, ver. 3, August 4, 2006. The EUCOM proposal had the GCC as the supported command for all NetOps, and the SGNOSCs in direct support of the component 6's vice the JNOC.

58. U.S. Department of Defense, National Defense Strategy of the United States of America (Washington DC: U.S. Department of Defense, March 2005), 14.

59. Clark A. Murdock, et al., *Beyond Goldwater-Nichols: U.S. Government and Defense Reform for a New Strategic Era* Phase 2 Report (Washington DC: Center for Strategic and International Studies, July 2005), 82, 85-86.

60. General Peter J. Schoomaker, *Serving a Nation at War: A Campaign Quality Army with Joint and Expeditionary Capabilities* (Washington DC: U.S. Army Public Affairs, Army Strategic Communications, June 29, 2004), 19.